# Basic Computer Security

# **Outline**

☞ Why Computer Security
☞ Fermilab Strategy:
 – Integrated Computer Security
 – Defense in Depth
☞ Your role and responsibilities as a user
☞ Other Computing Policy Issues
 – Data backup
 – Incidental use
 – Privacy
 – Offensive material
 – Licensing

# Why Computer Security

☞ The Internet is a dangerous place
  – We are constantly being scanned for weak or vulnerable systems; new unpatched systems will be exploited within minutes.

☞ Fermilab is an attractive target
  – High network bandwidth is useful for attackers who take over lab computers
  – Publicity value of compromising a .gov site
  – Attackers may not realize we have no information useful to them

# Why Computer Security - 2

* We need to protect
  - Our data
  - Our ability to use our computers (denial of service attacks)
  - Our reputation with DOE, Congress and the general public
* Major sources of danger
  - Running malicious code on your machine due to system or application vulnerabilities or improper user actions
  - Carrying infected machines (laptops) in from off site

# FNAL Strategy

☞ Integrated Security Management
☞ Defense in Depth
   – Perimeter Controls and auto blocking
   – Mail gateway virus scanning
   – Central Authentication (Kerberos)
   – Major Applications with enhanced security concerns
   – Patching and configuration management
   – Critical vulnerabilities
   – Prompt response to computer security incidents (FCIRT)
   – Intelligent and informed user community

# Integrated Security Management

- Computer Security is not an add-on or something external, it is part and parcel of everything you do with computers (analogy with ES&H)

- Not "one-size-fits-all", but appropriate for the needs and vulnerabilities of each system

- In most cases, it is simply common sense + a little information and care

- Each Division/Section or large experiment has a GCSC (General Computer Security Coordinator) who acts as liaison with the Computer Security Team in disseminating information and dealing with incidents; see **http://security.fnal.gov/** for an up to date list

# Perimeter Controls

) Certain protocols are blocked at the site border (email to anything other than lab mail servers; web to any but registered web servers; other frequently exploited services)

) Temporary (automatic) blocks are imposed on incoming or outgoing traffic that appears similar to hacking activity; these blocks are released when the activity ceases (things like MySpace and Skype will trigger autoblocker unless properly configured)

# **Central Authentication**

- ☞ All use of lab computing services requires central authentication
- ☞ Avoid disclosure of passwords on the network
- ☞ No network services (logon or read/write ftp) visible on the general internet can be offered with out requiring strongest authentication, currently Kerberos (unless a formal exemption is applied for and granted)
- ☞ Kerberos provides a single sign in, minimizing use of multiple passwords for different systems
- ☞ Lab systems are constantly scanned for violations of this policy

# Major applications

- Defined as "critical to the mission of the Laboratory", i.e. disruption may have major impact on Laboratory operations; these require moderate level security controls (as opposed to the lab baseline low level controls)
  - Most things do *not* fall in this category;
- Special (more stringent) rules & procedures apply; each MA has its own security plan with enhanced and compensatory security controls beyond the baseline security controls. (Some "Minor Applications" will also have their own security plans.)
- You'll know if you're in this category;

# Grid Security Training

☞ If you are:

- a system administrator of systems that accepts grid jobs (generally jobs that are authenticated by credentials other than standard Fermilab Kerberos credentials); or
- a system administrator of one of the associated systems that provides support for the Fermi Grid infrastructure (such as GUMS and VOMS servers); or
- a developer of grid middleware software

then in addition to this course you require the training course entitled
"Security Essentials for Grid System Administrators"
which is available both in face to face sessions and online.

☞ If you are a user of grid computing resources you require the training course about PKI Authentication

# Patching and Configuration Management

☞ Baseline configurations exist for each major operating system (Windows, linux, MAC)

☞ All systems must meet the baseline requirements and be regularly patched (in particular running an up-to-date supported version of the operating system) UNLESS:

– A documented case is made as to why the older OS version cannot be upgraded

– Documentation exists to demonstrate that the system is patched and managed a securely as baseline systems

– All non essential services (such as web servers) are turned off

☞ All systems with Windows file systems must run anti virus

☞ Your system administrator should take care of this for your desktop

# Critical Vulnerabilities and Vulnerability Scanning

☞ Certain security vulnerabilities are declared critical when they are (or are about to) being actively exploited and represent a clear and present danger

☞ Upon notification of a critical vulnerability, systems must be patched by a given date or they will be blocked from network access

☞ This network block remains until remediation of the vulnerability is reported to the TISSUE security issue tracking system (as are blocks imposed for other security policy violations)

# Computer Security Incidents

☞ Mandatory incident reporting;

  – Report all suspicious activity:

    • *If urgent* to FCC Service Desk, x2345, 24x7;

    • *Or* to system manager (if immediately available);

    • Non-urgent to computer_security@fnal.gov;

  – Incidents investigated by Fermi Computer Incident Response Team (FCIRT);

  – *Not* to be discussed!

# FCIRT (Fermi Computer Security Incident Response Team)

) Security experts drawn from throughout the lab

) Investigate ("triage") initial reports;

) Coordinate investigation overall;

) Work with local system managers;

) Call in technical experts;

) May take control of affected systems;

) Maintain confidentiality;

# Mandatory System Manager Registration

☞ System managers must be registered with FCSC

☞ This is the person responsible for configuring your system and installing patches (probably not you, but you should know who this person is)

☞ Go to http://security.fnal.gov and click on "verify your node registration" to see who is registered as sysadmin for your system

# Prohibited Activities

- "Blatant disregard" of computer security;
  - First time perhaps only warning, repeat offense disciplinary action;
- Unauthorized or malicious actions;
  - Damage of data, unauthorized use of accounts, denial of service, etc., are forbidden;
- Unethical behavior;
  - Same standards as for non-computer activities;
- Restricted central services;
  - May only be provided by approved service owners;
- Security & cracker tools;
  - Possession (& use) must be authorized;
- See http://security.fnal.gov/policies/cpolicy.html

# Your role as a user

☞ Guard against malicious code in email
  – Don't open attachments unless you are sure they are safe
  – Don't trust who email is from
  – Updated and enabled virus signatures
☞ Guard against malicious code from web browsing
☞ Watch out for "social engineering" (someone obtaining your password through trickery rather than hacking)

# Your role - 2

☞ Obey Central Authentication Policy (Kerberos)

  – Don't run network services (login or read write ftp) unless they demand Kerberos authentication

  – Treat your kerberos password as a sacred object (never expose it over the network)

☞ Promptly report potential computer security incidents

  – X2345 or computer_security@fnal.gov

  – Follow FCIRT instructions during incidents (especially about keeping infected machines off the network and preserving the status of an infected machine for expert investigation)

# Other Computing Policy Issues

☞ Data backup

☞ Incidental use

☞ Privacy

☞ Offensive material

☞ Licensing

# Data Backup Policy - Users

- Users (data owners) responsible for determining:
    - What data requires protection;
    - How destroyed data would be recovered, if needed;
    - Coordinating backup plan w/ sysadmins;
        - or doing their own backups;
    - If the backup is done for you it might be worth occasionally checking that you can really retrieve the data

# Incidental Computer Usage

☞ Fermilab permits some non business use of lab computers

☞ Guidelines are at http://security.fnal.gov/ProperUse.htm

# Activities to Avoid

☞ Large grey area, but certain activities are "over the line";

- Illegal;
- Prohibited by Lab or DOE policy;
- Embarrassment to the Laboratory;
- Interfere w/ performance of job;
- Consume excessive resources;

☞ Example: P2P (peer to peer) software like Skype and BitTorrent: not explicitly forbidden but very easy to misuse!

# Privacy of Email and Files

☞ Fermilab normally respects the privacy of electronic files and email;

☞ Employees and users are required to do likewise;

☞ Certain exemptions for system managers and computer security response;

☞ All others *must* have Director(ate) approval;

# Privacy of Email and Files

) May not use information in another person's files seen incidental to any activity (legitimate or not) for any purpose w/o either explicit permission of the owner or a "reasonable belief the file was meant to be accessed by others."

– Whether or not group/world accessible;

– "Group" files implicitly may be used by the group for the mission of the group;

# Offensive Material on computers

☞ Many "computer security" complaints are not;

☞ Material in a computer is like material in a desk;

 – With respect to both privacy and appropriateness;

☞ This is a line management, not computer security, concern (except in egregious cases).

# Software Licensing

☞ Fermilab is strongly committed to respecting intellectual property rights

☞ Any use of unlicensed commercial software is a direct violation of lab policy

# Summary: User Responsibilities

☞ Appropriate use of computing resources

☞ Prompt incident reporting

☞ Proper Information handling (see Protecting Personal Information course)

☞ Know how your data is backed up

☞ Receive computer security training

☞ Respect privacy of electronic information

# Summary: System Admin Responsibilities

) System registration

) Virus protection, patching and configuration management

) Access control: telnet an ftp type services require kerberos authentication

) Do not offer any of the restricted central services

# **Questions?**

☞ [nightwatch@fnal.gov](mailto:nightwatch@fnal.gov) for questions about security policy

☞ [Computer_security@fnal.gov](mailto:Computer_security@fnal.gov) for reporting security incident

☞ [http://security.fnal.gov/](http://security.fnal.gov/)